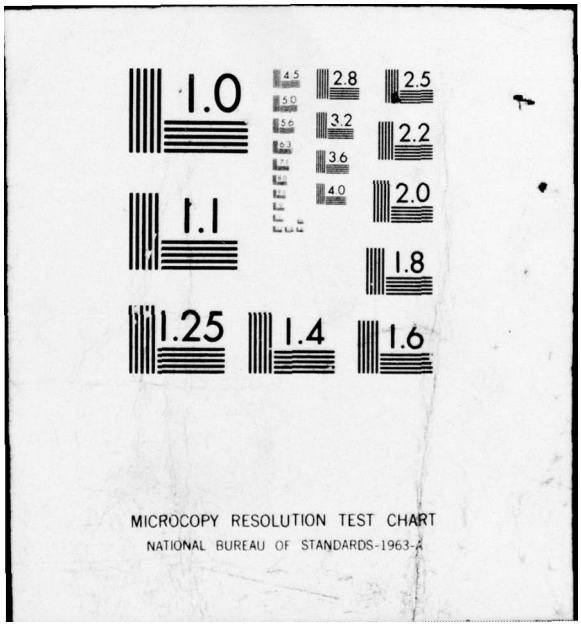
AD-A031 668 RAND CORP SANTA MONICA CALIF F/G 17/2
PRIVACY SYSTEMS FOR TELECOMMUNICATION NETWORKS,(U)
SEP 74 R TURN
UNCLASSIFIED P-5292 NL

| OF |
AD
A031 668

END
DATE
FILMED
12-76


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

(2) FC

(6) PRIVACY SYSTEMS FOR TELECOMMUNICATION NETWORKS

(10) Rein/Turn

(11) September 1974

(12) 8p.

(14) P-5292

The Rand Corporation
Santa Monica, California 90406

PRIVACY SYSTEMS FOR TELECOMMUNICATION NETWORKS

Rein Turn
The Rand Corporation
Santa Monica, California 90406

ABSTRACT

There is an increasing need for providing privacy and security in telecommunication and teleprocessing networks. This paper presents a brief survey of privacy systems--the techniques that can be used to provide communications security in commercial systems--and then examines in qualitative terms the protective characteristics of several classes of privacy transformations (encryption techniques). The emphasis is on the level of protection that can be expected and the effects of the telecommunication network characteristics on the performance of the privacy system, and vice versa.

INTRODUCTION

The explosive growth of computer technology in the last two decades has been parallelled by similar advances in telecommunications. Indeed, the two technologies appear to be on the path toward merging into a single teleprocessing technology. In this new technology there are added to the traditional man-to-man communications also man-to-machine and machine-to-machine communications. As a result, the widely used analog communication systems are being augmented and gradually replaced by digital techniques and systems. The latter have permitted introduction of new concepts, such as packet communications and store-and-forward transmission techniques. New components have emerged, such as digital switching centers, communications processors, and more capable communications terminals [1,2].

The innovations in the telecommunication system design and operation provide more communications capacity, efficiency, quality, and economy. This has permitted the construction of large teleprocessing systems where computers may be accessed from terminals anywhere in the country. The National Crime Information Center (NCIC), various reservation systems, management information systems of many large corporations, and teleprocessing services for commercial subscribers are examples.

Nearly all such systems communicate, process, and store information which is considered private by their owners and users, or which must be safeguarded from unauthorized access as required by law. The new digital telecommunications systems are not changing the fact that in any telecommunication channel the messages are not under the direct control of the sender or the intended receiver, and that they can be overheard or intercepted by anyone who has the appropriate equipment and knowhow [3,4]. Therefore, if the content of a message is to remain known only to the sender and the receiver, *special protective techniques* must be applied by the communicators or provided by the telecommunication systems, i.e., *privacy systems* must be designed and implemented.

In addition to protecting messages from unauthorized accidental or deliberate overhearing or interception, there is also a need to protect the communication system against *active* infiltration--the insertion into the system of unauthorized messages. The purpose of the latter may be to request the information desired by the intruder (rather than passively monitor the communication lines and hope that the desired information will appear), to insert false information, or to disrupt the operation of the communication network or the systems that it serves. For example, in the telecommunications links serving remote computer terminals or computer networks, there exists the threat that illicit terminals or computers may be connected to the network for the purposes of "managing" the normal terminal-computer communications, masquerading as a legitimate user, or simply making the system unavailable to its users [5,6].

*This paper was prepared for presentation at the 1974 IEEE National Telecommunications Conference, San Diego, California, December 2-4, 1974.

This paper reviews the relevant characteristics of several classes of privacy systems, discusses a set of suitability criteria for their application in teleprocessing systems, and concludes with a discussion of their implementation and operation considerations.

PRIVACY SYSTEMS

A need for maintaining confidentiality of communications has existed from the days of antiquity and, indeed, the ancient Greeks and Romans deserve a great deal of credit for furthering the art of secret writing--cryptography [7,8]. With the invention of telegraph, telephone and radio there also arose a need to provide privacy protection to electrically and electronically transmitted messages.

Shannon [9] distinguishes three types of protective systems:

- *Concealment systems* which attempt to hide the very existence of a message (e.g., use of invisible ink, or mixing a message with unrelated text or dummy messages);
- *Privacy systems* which require special equipment for recovering the message (e.g., speech inversion systems);
- *Secrecy systems* where the existence of a message is not hidden but its content is concealed by a cipher or a code, and where the equipment for its interception is assumed to be available for the would-be intruders.

In the following only the last two types are considered and they are collectively referred to as *privacy systems*. Although a large amount of telecommunication traffic consists of voice communications where messages are represented by time-varying analog signals, privacy systems have been developed almost exclusively for sequences of discrete symbols--characters of the message alphabet, and their representations in telecommunication systems. Thus, they are especially suitable for protecting digital data or digitized voice communications.

A privacy system operates as follows: The sender composes a message M, using the vocabulary, syntax, grammar, and alphabet A, of a natural or artificial language L. He then applies a transformation T(K) which changes (encrypts, enciphers) the message M (the cleartext) into a transformed form E (the ciphertext or cryptogram). The ciphertext E is then transmitted to the receiver over the communication channel. The transformation T(K) is chosen from a large set of all such transformations by specifying the value of K, the *key* of the transformation. The key is also transmitted to the intended receiver using a secure and uninterceptable channel. The receiver applies to E the inverse transformation $T(K)^{-1}$ and recovers (decrypts, deciphers) the original message M. The degree of protection provided by such a privacy system depends on the type of transformations used, the ability of the transformations to obscure the characteristics of the language L, and the number keys that can be used.

In *voice communication* links that use analog signal transmission the transformation T(K) may be one of the following: (1) a simple frequency inversion of the voice signal, (2) alternating inversion under the control of a pseudo-random sequence, (3) spectrum shifting, or (4) band splitting [10]. These techniques provide varying degrees of privacy by distorting and scrambling the voice signal. Transmission of voice in *digital form* permits the treatment of voice signals as sequences of discrete symbols and, thus, allows application of the privacy transformations as discussed in the following sections of this paper. The digitization process itself, such as in the case of vocoders [11], provides a degree of privacy against accidental overhearing, but not against determined intruders who have the appropriate equipment available.

The future telecommunication systems will be all-digital and will permit simultaneous transmission of data and digitized voice. Therefore the rest of this examination of privacy systems deals with telecommunication networks where the messages are composed of discrete symbols and signals.

PRIVACY TRANSFORMATIONS

Numerous types of privacy transformations have been proposed and used in privacy systems [12,13]. Basically, all transformations perform *substitution operations on the message M*. That is, a segment m of one or more symbols of the message M is replaced by a set, e, of symbols to form E, the *ciphertext* corresponding to M. The segment e need not contain the same number of symbols as the segment m, and the symbols used in e may be different from those in m (i.e., the ciphertext alphabet or alphabets may be different from the message alphabet A).

The basic differences between various types of privacy transformations are in the number of symbols in m, the number of symbols in e, and the functional relationship between the segments e and m. Thus,

- *Monographic substitutions.* In this class one symbol of M is operated on at a time (m=1) and is replaced with one or more symbols ($e \geq 1$).
- *Polygraphic substitutions.* Two or more symbols of M are operated at a time and replaced by a similar or larger group of symbols ($m \geq 2$, $e \geq 2$).

Both families contain several classes of transformations. The principal monographic substitutions are:

- *Monoalphabetic* substitutions where corresponding to each symbol, a_i, of the message alphabet A there is a fixed symbol, b_j, of the ciphertext alphabet B. Usually B is a permutation of A. One very simple transformation, the Caesar cipher, is obtained when B is a cyclic permutation of A.
- *Polyalphabetic* substitutions use n ciphertext alphabets, $B_1, \ldots, B_n$, to replace symbols of the message alphabet A. The alphabets are used cyclically with a period n. Usually the alphabets B_j are permutations of A, and not all B_j need to be distinct. The key specifies the number of alphabets used and their sequence. A special case is the Vernam cipher where the number of alphabets used, n, is longer than the number of symbols in the message.
- *Homomorphic* substitutions [14] where the transformation is monoalphabetic for some symbols of the message alphabet A and polyalphabetic (with different periods) for other symbols of A. The choice is usually associated with the average frequency of occurrences of symbols in the language L that is used--polyalphabetic transformations are used for the more frequently occurring symbols.

Among the *polygraphic* transformations are substitutions of symbol groups of the message M with other symbol groups from a single substitution table (as in monoalphabetic substitutions) or from several cyclically used substitution tables (as in polyalphabetic substitutions). Another important class of transformations in this family are:

- *Transpositions* where the segments m of the message M are operated upon by permuting the symbols within each segment according to some rule specified by the key.

The choice of a particular class of privacy transformations for use in a given telecommunication network depends on the level of protection desired and the performance requirements of the network. For higher levels of protection, messages may be transformed several times before transmission by using different types of transforms. For example, one can apply *block transforms* where fixed, relatively long segments of the message are subjected to transpositions and substitutions [15].

Two other techniques used in telecommunication systems, coding and data compression, can also provide privacy protection. *Coding* is a transformation where an entire message, sentence, words or syllables of the language L are replaced with groups of characters of some other (usually artificial) language[7,16]. The coding transformation and its inverse, the decoding transformation, are performed with the help of a codebook that establishes the correspondences between the expressions in languages L and L'. A high level of protection can be provided. In addition, coding also provides a great deal of message compression. Indeed, this was the original objective in introducing coding systems.

Other *message compression* techniques are based on removing redundancy in the natural language or in data to be transmitted in order to reduce transmission time or bandwith requirements [17,18]. The transformations used on natural language messages involve elements of coding and removal of characters of the original text in such a way that the original can be restored by using the context of the message. In data, consecutive occurrences of the same symbol (e.g., 0 or blank) can be replaced by an expression that specifies the symbol and the number of times of its consecutive occurrences in the original message. Privacy protection is not the main purpose of compression but a certain low level of protection will be provided by the distortions introduced by the compression algorithms.

SUITABILITY CRITERIA

The suitability of a class of privacy transformations in a given telecommunication system application depends on the amount of protection desired, the effects of the transformations on the communication system's performance and characteristics, and the cost of implementing and operating the privacy system. Over ninety years ago, Auguste Kerckhoffs [19] formulated a set of criteria that should be satisfied by any privacy system that may be summarized as follows: (1) The privacy system used should be, if not theoretically unbreakable, unbreakable in practice; (2) A knowledge by the "enemy" of the privacy system's hardware and techniques must be assumed, but this knowledge should not compromise the level of protection provided. That is, the key of the transformation should be able to provide all of the protection; (3) The key should be remembered without notes and should be easily changeable. The transformations should be easy to apply, neither requiring the knowledge of a long list of rules nor involving mental strain.

The last requirements reflect the manual application of privacy transformations in Kerckhoffs' days. In modern telecommunication systems, there should be no need for a user to know the key nor personally apply the transformations--advances in microelectronics technology allow equipping communications terminals with sufficient processing capability to apply very complex transformations [20].

Amount of Security

A necessary but not sufficient prerequisite for an effective privacy system is a large *key space*--a very large number of possible keys such as to make impractical any trial and error search for the key. With the exception of the Caesar cipher, all classes of transformations discussed above have the potential for satisfying this requirement. The size of the key space for the Caesar ciphers, however, is one less than the number of symbols in the message alphabet A (e.g., 25 for the 26-character English alphabet).

The classical approach to breaking privacy systems is based on the statistics of the message language L and on some knowledge of the probable content of the messages [21,22]. The principal statistics used are (1) the average frequencies of individual symbols of the alphabet A,(2) digram and k-gram frequencies, (3) word frequencies, (4) character patterns in words, and (5) the grammatical and syntactic rules. A knowledge of the *context* of the messages allows postulating probable words, expressions and formats used. For natural languages these statistics are well established and can be quite revealing. For artificial languages and numerical data, however, statistics are more dependent on the context and hence, less predictable. In these cases information on the syntactic structures and formats may be more useful.

Given the language statistics and sufficient amount of ciphertext, monoalphabetic substitutions are solved easily since they leave all language statistics invariant--they only change the alphabets used. Polyalphabetic transformations will change all language statistics, but not the syntactic structure. However, if the number of alphabets (the key period), is known and a string of 50n characters of ciphertext is available (for English) the system can be analyzed as if it were n monoalphabetic substitutions [9]. In the case of Vernam cipher where n is larger than the message length and a key is never used more than once, the privacy system is theoretically and practically unbreakable.

A transposition transformation over k characters leaves the character frequencies intact but distorts the higher order language statistics and the syntactic structure. Although techniques for breaking transposition transformations have been developed, much more effort is required than for substitution transformations. At least 1.7 logk! ciphertext characters must be available [9].

Large volumes of message traffic in a communication network may lead to practices which can significantly augment the classical cryptanalytic approaches and reduce the effectiveness of the privacy system. Examples of information that helps cryptanalysis include (1) A number of different messages are known to be transformed using the same key--these can be used for simultaneous solution for the key and checking of the trial solutions; (2) Fragments of the message, or paraphrased versions of the message are published after its transmission in ciphertext form. These are very useful for generating trial solutions. (3) The key selection practices of the privacy system may be known. For example, if the keys are short they may be selected to be words in a natural language or names, rather than totally random character groups; (4) Fragments of the key itself may be available or can be deduced from a

knowledge of the message composition and formatting practices.

Given this information, techniques can be devised for breaking any privacy system. Tuckerman [23] has shown that if a fragment of the message longer than the key period is available (even though its location in the ciphertext is unknown) the key can be readily determined by algebraic and heuristic techniques. Further, if the key of a polyalphabetic substitution is produced by a pseudorandom process (e.g., n-stage feedback shift register) and applied as bit-by-bit addition of the key to the message [24], a message fragment of only 2n bits is sufficient for breaking the key [25]. However, if complex sequences of transpositions and substitutions are applied [9, 15,20] the system may be able to withstand cryptanalysis for very long periods of time even though message fragments are available. If this time is longer than the time for the messages to lose their value, an effective privacy system has been achieved.

Performance

Also important in the design of privacy systems are the effects of communication channel errors on the privacy system, and the effects of the privacy system on the communication network performance. Transformations that use previously generated ciphertext as the key (e.g., the "auto-key" systems [7] and certain block ciphers) tend to amplify the effects of channel errors in the decryption process. As a result, the original message may be unrecoverable and must be retransmitted. If errors persist, the frustrated communicators may decide to transmit the message in the clear and, thus, provide valuable material for breaking the key. Indeed, quite a few military cryptographic systems have been broken in this fashion.

One answer to the channel error problem is the use of errorcorrecting codes superimposed on the ciphertext. However, the simple substitution and transposition transformations operate on each character independently and do not amplify errors.

The effects of privacy transformations on the length of the message and on the message transmission time are other items of concern--they affect the bandwidth required. The message length is increased in privacy systems where polygraphic substitutions are made or where the ciphertext alphabets are considerably longer than the message alphabet (i.e., more bits are required to represent a character). Complex block transformations may also increase the ciphertext length and encryption time.

IMPLEMENTATION

Two basic privacy system structures can be used in communication systems: end-to-end encryption, and link-by-link encryption [26]. In the first structure, all sender-receiver pairs use agreed-upon keys and perform the transformations at their own terminals. In large networks with many subscribers, end-to-end systems pose cumbersome problems with the keys:For high security, each pair of communicators should use different keys and the keys should be changed often (on-time keys would be ideal). The distribution and storage of large number of keys can seriously affect the effectiveness of the privacy system.

A link-by-link encryption system can be implemented in packet switching communication networks or in those that use other store-and-forward message transmission and routing techniques. Such networks consist of switching nodes and node-to-node transmission channels. A different privacy transformation can be applied to each link. A user needs to handle only one key--the key used in the link between his terminal and the node that serves the terminal. One disadvantage is the need to decrypt and re-encrypt the messages at each node. In order to avoid storage of the messages being routed in the clear, the communications processor at a node should immediately apply its own internal transformation.

In order for a privacy system at a terminal to match the performance requirements of modern communications, it is necessary to apply the privacy transformations automatically by using special devices. The earliest "cipher machines" used by the governments were electromechanical units equipped with randomly wired rotors that implemented polyalphabetic substitutions with extremely long key periods [7]. The presently available commercial devices are usually based on feedback shift-register key stream generators whose vulnerability problems were mentioned previously. An important requirement for their use is the *synchronization* of the key generators at the transmitter and at the receiving terminal. If synchronization is lost, the message cannot be recovered and must be retransmitted.

Transpositions and block ciphers require more complicated hardware for storing the message segment being encrypted and applying the transformation rules. However, modern microcircuit technology permits the construction of small circuit packages that can hold a large amount of memory and logic circuits. For example, the IBM's ciphering device "Lucifer" [20] is estimated to require only four large scale integrated

(LSI) circuit chips for applying a block cipher to 128-bit message segments. No synchronization is needed.

Finally, communication networks use various signals for network control purposes. Application of privacy transformations to messages is likely to produce inadvertent control characters in the ciphertext. It is necessary, therefore, to make provisions in the network control circuits for distinguishing bona fide control signals from those in the ciphertext. The other alternative--suppression of control characters in the ciphertext--seems more difficult to implement.

CONCLUDING REMARKS

The need for security in telecommunication networks is increasing. Privacy transformations can provide protection against many threats: misrouting of messages, wiretapping, active entry through illicit terminals, and disruption of operations by illicit messages. Several classes of privacy transformations are available, but they are not equally effective. In particular, a large number of available keys does not mean a high degree of protection.

Recent advances in the manufacture of LSI circuits will permit economic implementation of privacy systems that use very complex block transformations and can provide any desired level of protection without penalizing the performance of the associated telecommunication network.

REFERENCES

1. J. Martin, *Telecommunications and the Computer*, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1969.
2. D. W. Davies,"Packet Switching, Message Switching and Future Data Communications Networks," *Information Processing 74*, North-Holland Publishing Co., Amsterdam, 1974, pp. 147-150.
3. J. M. Carroll, *The Third Listener*, E. P. Dutton & Co., New York, 1969.
4. "Taps to Steal Data," *Security World*, December 1972, pp. 45-46.
5. H. E. Petersen and R. Turn, "Systems Implication of Information Privacy," *Proceedings 1967 SJCC*, pp. 291-300.
6. J. M. Carroll and P. Reeves, "Security of Data Communications: A Realization of Piggyback Infiltration," *Infor*, October 1973, pp. 226-231.
7. D. Kahn, *The Codebreakers*, The MacMillan Co., New York, 1967.
8. A. C. Leighton, "Secret Communications Among the Greeks and Romans," *Technology and Culture*, April 1969,pp.139-154.
9. C. E. Shannon, "Communications Theory of Secrecy Systems," *BSTJ*, 1949, pp. 656-715.
10. R. L. Carlson and J. M. Schreiber, "Privacy of Voice Communications," *Security World*, May 1972, pp. 48-53.
11. M. R. Schroeder, "Vocoders," *Proceedings IEEE*, May 1966, pp. 720-734.
12. G. E. Mellen, "Cryptology, Computers and Common Sense," *Proceedings 1973 NCC*, pp. 569-579.
13. A. Sinkov, *Elementary Cryptanalysis*, Random House, New York, 1968.
14. F. A. Stahl, "A Homomorphic Cipher for Computational Cryptography," *Proceedings, 1973 NCC*, pp. 565-568.
15. H. Feistel, W. L. Notz and J. L. Smith, "Cryptographic Techniques for Machine-to-Machine Data Communications," RC-3663, IBM Research Labs, Yorktown Heights, N. Y., December 27, 1971.
16. W. P. Friedman and G. J. Mendelsohn, "Notes on Code Words," *American Mathematical Monthly*, August 1932, p. 394.
17. H. E. White, "Printed English Compression by Dictionary Encoding," *Proc. IEEE*, March 1967, pp. 390-395.
18. S. S. Ruth and P.J. Kreutzer, "Data Compression for Large Business Files," *Datamation*, September 1972, pp. 62-66.
19. R. O. Skatrud, "A Consideration of the Application of Cryptographic Techniques to Data Processing," *Proceedings 1969 FJCC*, pp. 111-117.
20. W. L. Notz and J. L. Smith, *An Experimental Application of Cryptography to a Remotely Accessed Data System*, RC-3508, IBM Research Labs, Yorktown Heights, N.Y., August 18, 1971.
21. R.Turn, "Privacy Transformations for Databank Systems," *Proceedings 1973 NCC*, pp. 589-601.
22. G. A. Miller and E. A. Friedman, "The Reconstruction of Mutilated English Texts," *Information and Control*, 1957, pp. 38-55.
23. B. Tuckerman, *A Study of the Vigenere-Vernam Single and Multiple Loop Enciphering Systems*, RC-2879, IBM Research Labs, Yorktown Heights, N.Y., May 14, 1970.
24. E. S. Donn, "Secure Your Digital Data," *The Electronic Engineer*, May,1972, p.5.
25. C.H. Meyer and W. L. Tuchman, "Pseudo-random Codes Can Be Cracked," *Electronic Design*, November 9, 1972, pp.74-76.
26. P. Baran, "On Distributed Communications: Security, Secrecy, and Tamper-Free Considerations," in L.J.Hoffman (Ed.), *Security and Privacy in Computer Systems* Melville Publishing, Los Angeles, 1973.